IDS - We're Doing It Wrong

Shane Biggins

BAE Systems Stratsec

Who is this guy anyway?

Shane Biggins, Business Analyst

BAE Systems Stratsec Capability Development

- BAE Systems, Tech Lead for operations seven + years
  - Investigating data spills on classified systems.
- Cyber Support Unit
  - Secured funding for new line of business
  - Retooling Defence capability for larger audience.
- Plus61.org
- BAE Systems Stratsec

Definition

(Network) Intrusion Detection System:

1. Sensor on the network
2. Rules-engine to detect suspicious traffic
3. Generates Alerts

3

Landscape I: PWNED!!

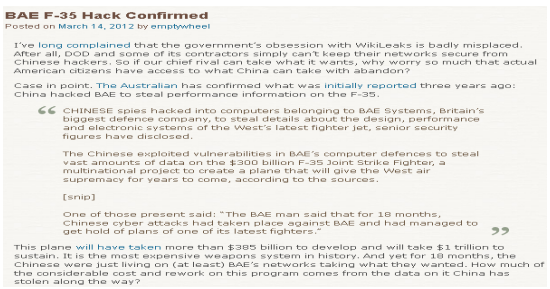
Security tech has never been better


Open Letter to RSA Customers

Arthur W. Coviello, Jr.

Like any large company, EMC experiences and successfully repels multiple cyber attacks on its IT infrastructure every day. Recently, our security systems identified an extremely sophisticated cyber attack in progress being mounted against RSA. We took a variety of aggressive measures against the threat to protect our business and our customers, including further hardening of our IT infrastructure. We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities.

Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). Our investigation also revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is specifically related to RSA's SecurID two-factor authentication products. While at


BAE F-35 Hack Confirmed

Posted on March 14, 2012 by emptywheel

I've long complained that the government's obsession with WikiLeaks is badly misplaced. After all, DOD and some of its contractors simply can't keep their networks secure from Chinese hackers. So if our chief rival can take what it wants, why worry so much that actual American citizens have access to what China can take with abandon?

Case in point. The Australian has confirmed what was initially reported three years ago: China hacked BAE to steal performance information on the F-35.

> CHINESE spies hacked into computers belonging to BAE Systems, Britain's biggest defence company, to steal details about the design, performance and electronic systems of the West's latest fighter jet, senior security figures have disclosed.
>
> The Chinese exploited vulnerabilities in BAE's computer defences to steal vast amounts of data on the $300 billion F-35 Joint Strike Fighter, a multinational project to create a plane that will give the West air supremacy for years to come, according to the sources.
>
> [snip]
>
> One of those present said: "The BAE man said that for 18 months, Chinese cyber attacks had taken place against BAE and had managed to get hold of plans of one of its latest fighters."

This plane will have taken more than $385 billion to develop and will take $1 trillion to sustain. It is the most expensive weapons system in history. And yet for 18 months, the Chinese were just living on (at least) BAE's networks taking what they wanted. How much of the considerable cost and rework on this program comes from the data on it China has stolen along the way?

But still not keeping us out of the papers

4

Landscape II: Damage != Sophistication

Some people just want to see the world burn

Technology

News | Security | Sci-Tech | Blogs | IT Pro | Digital Life | Compare & Save

You are here: Home » Technology » Security » Article »

4800 Aussie sites evaporate after hack

Asher Moses
June 21, 2011

★Read later | Comments 106

Join the conversation
You're the only person reading this now. Tell your friends
106 comments
Recommend 890
Tweet 486

"I think I'm in shock ... I have lost everything .... I couldnt possibly replicate all those years of work again."

Related Coverage
Thousands of Aussie websites exposed in hack attack
17 JUN | Thousands of Australian

Ads by Google
Free Forex Guide www.GFT.com.au
Four Simple Steps to Making Your First Spot Forex Trade. Start Here.

At least 4800 Australian websites have been lost with no chance of recovery following a break-in at Australian domain registrar and web host Distribute.IT.

The hack attack caused so much damage that four of the company's servers were "unrecoverable", the company said, leaving thousands of website owners in the lurch.

"The overall magnitude of the tragedy and the loss of our information and yours is simply incalculable; and we are distressed by the actions of the parties responsible for this reprehensible act," Distribute.IT said.

Critical that you 'know thyself'

5

Landscape III: Not enough ninjas!

Difficult to resource your security

in an employees market.

6

Tools I: Intrusion Detection Systems

Key Component of our Defence-In-Depth Strategy

1. **Natural habitat is the perimeter**
2. **Rule-based (if X then Y)**
3. **Stateless and pressed for time.**

7

Tools II: Intrusion Detection Systems

Characteristics

1. **Box-drop culture**
2. **Needy**
3. **Noisy by nature**

8

The long tail of analysis

We still need humans to make determinations.

9

The IDS Conundrum

We have more alerts than we can deal with…

And we can't staff them properly.

10

Potential Solutions

1. Reduce the noise (volume reduction)
2. Centralisation (the cloud? *Hisssssss!!!*)
3. Smarter Tools for Analysis

11

First line triage

Managing volume

12

Getting our tools right

Relationship modelling to:

1. **Provide analysts with all they need for rapid triage**
2. **Detect subtle patterns, particularly across time**
3. **Use extra information to reduce false positives**

What can be done automatically?

13

Enriching the Analytics

Prioritisation – don't leave home without it.

14

Enriching the Analytics

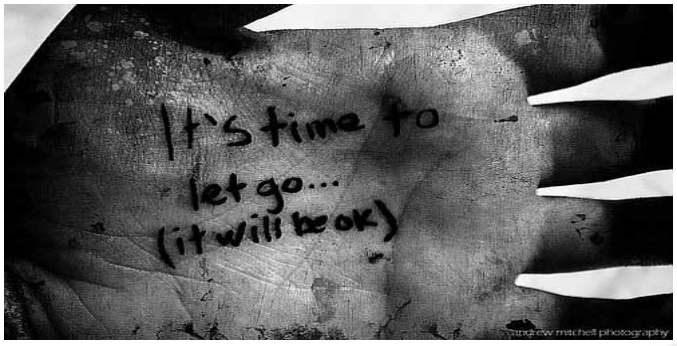
Better Living Through Contextual Analysis

Example 1: **Identical email sent individually to many recipients.**

Example 2: **Periodic Beckoning**

15

The (Imaginary) Trade off.



Letting go of real-time

16

Summary: Tips from the Wounded.

1. Tools are the means not the ends.
2. Forget line-speed analysis.
3. Resourcing: an untended IDS is a waste of budget.
4. Massive efficiency gains come from getting prioritisation right.

17

Thank You

shane.biggins@baesystems.com

Adelaide:
T: +61 8 8300 4400
F: +61 8 8349 7420
A: 2 Second Avenue, Tech Pk, Mawson Lakes SA 5095

Canberra
T: +61 2 6260 8878
F: +61 2 6260 8828
A: Suite 1, 50 Geils Court, Deakin ACT 2600

Perth
T: 1300 027 001
F: +61 2 6260 8828
A: PO Box 8163, Angelo Street, South Perth WA 6151

Melbourne
T: 1300 027 001
F: +61 3 9614 4760
A: Level 1, 2 Queen Street, Melbourne VIC 3000

Sydney
T: 1300 027 001
F: +61 2 9251 6393
A: Level 6, 62 Pitt Street, Sydney NSW 2000

18